TITLE

COPY PROTECTION SYSTEM FOR PORTABLE STORAGE MEDIA

CLAIM FOR PRIORITY

This application makes reference to, incorporates the same herein, and claims all rights accruing thereto under 35 U.S.C. §119 through our patent applications entitled *The Digital Content Encryption Apparatus And Method Thereof* earlier filed on the 24th day of September 1998 in the Korean Industrial Property Office and there duly assigned Serial Nos. 1998/39808 and 1998/39809.

FIELD OF THE INVENTION

The present invention is generally related to encryption processes and apparatus, and, more particularly, to secure and robust processes and apparatus for the generation and use of keys in the transmission and replay of digital information for licensed SDMI compliant modules such as personal computers and SDMI compliant portable devices in conjunction with Internet service content provider and certificate authority.

BACKGROUND ART

Recently, with the flood of information provided by various media such as broadcasting and press, an atmosphere has been created by the information providers who are interested in providing integrated information that covers all of the media. Other users want to selectively receive a specific

item of digital information from the entire spectrum of information available from a particular information provider (IP). Accordingly, a digital content transmission system has been formed by the information providers who convert various types of information into digital form and store this digital information, and the users who subscribe to this digital information system from the information provider via the network. Digital information transmission systems endow an application program with easy downloadability of the digital content. The user can get all the information desired by using this application program to access the digital information system through the network.

The digital information may be provided to the user either for pay or for free. In case of paid digital information, the server who provide the digital information via the transmission system sets the service fee. The service server charges the user according to the quantity of information used when the digital information is downloaded to the user. MPEG software protocol for example, compresses audio files to a fraction of their original size, but has little perceptible affect upon the quality of the audio sound. MPEG software protocol is now widely used by Internet sites offering digitalized music, and is reported to be commonly used to offer digitalized versions of recorded music without the consent of the musicians. When a user is connected to a server that provides digital information commercially via a network, a few of the users may be able to inadvertently or illegally copy the digital information, a practice that, as was recently noted by Interdeposit and the French Agency for the Protection of Programs, a member of the European Association of Authors and Information Technology Professional, in the *Patent, Trademark & Copyright Journal*, volume 57, No. 1416, page 385 (11 March 1999), would be economically damaging to both the musicians

and to the server who is running the digital information transmission system. Currently, the server, as well as the musicians, can do little more than seek redress by undertaking civil and criminal action in an effort to control the possibility of unlicensed reception of digital information. We have noticed that there is a need for a technique to preserve transmission security of revenue bearing information while restricting access to the information by unauthorized entities and preventing unauthorized users from using any of the information that they may be able to illicitly obtain from the information provider by restricting the ability of the unauthorized users to decrypting whatever information they manage to obtain via the system.

SUMMARY OF THE INVENTION

It is therefore, one object of the present invention to provide improvements in cryptographic processes and apparatus.

It is another object to provide a secure and robust digital encryption process and apparatus.

It is yet another object to provide digital encryption processes and apparatus endowing a system with secure and robust copy protection for LCM's (*i.e.*, licensed SDMI (*i.e.*, secure digital music initiative) compliant modules such as personal computers) and PD's (*i.e.*, SDMI compliant portable devices such as disk and DVD players) in conjunction with ISP (*i.e.*, Internet service provider) and CA (*i.e.*, certificate authority).

It is still another object to provide digital encryption processes and apparatus able to encrypt and transmit digital information received from a transmission system, by the use of multiple cryptographic keys.

It is still yet another object to provide digital encryption processes and apparatus for generating and using multiple cryptographic keys during the transmission of digital information to a user.

It is a further object to provide digital encryption processes and apparatus that employ user information in the generation and use of multiple cryptographic keys during the transmission of digital information to the user.

It is a yet further object to provide digital encryption processes and apparatus able to encrypt and transmit digital information obtained from a transmission system by using multiple cryptographic keys, and to decrypt and play the digital information at the terminal of the user by using a plurality of keys, one of which is common to the multiple keys.

It is a still further object to provide digital encryption processes and apparatus able to encrypt and transmit digital information obtained from a transmission system by using key information, a user's key, and a temporary validation key, and to decrypt and play the digital information at the terminal of the user by using the key information and user authorization information.

It is still yet a further object to provide encryption, transmission and reception protocols enabling encryption, transmission and decryption of digital information received from a transmission system.

It is an additional object to provide encryption, transmission and reception protocols enabling encryption and transmission of digital information received from a transmission system by using multiple keys to encrypt the digital information, and decryption and replay of the digital information at the terminal of the user by using a plurality of keys, one of which is common to the multiple keys.

It is a still yet further object to provide encryption, transmission and reception protocols enabling encryption and transmission of digital information received from a transmission system, by using key information, a user's key, and a temporary validation key, and decryption and replay of the digital information at the terminal of the user by using the key information and user authorization information.

It is also an object to provide a more secure cryptograph and process for transmitting information to a terminal of a user who has requested the information.

It is also a further object to provide a cryptograph and process that reliably restricts the ability of a registered subscriber who has validly obtained information from an information provider, to deliver that information to another entity in a readily usable form.

These and other objects may be attained with an encryption process and apparatus that provides a secure and robust copy protection system for a licensed secure digital music initiative compliant modules such as personal computers and portable devices, in conjunction with Internet service providers and certificate authorities, by responding to a user's request for transmission of items of digital information to the user's terminal unit, by providing copy protection during downloading and during uploading of the digital contents. In order to prevent the digital contents from being copied illegally, a plurality of keys are generated and held by both the user and the digital content provider, and a secret channel is formed between both the user and the digital content provider. The header of the encrypted digital content is encrypted by using a physical address of a sector of a licensed SDMI compliant module such as a portable computer or a portable media device in order to prevent the digital content from being copied illegally after the digital content is recorded

in the portable media.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of this invention, and many of the attendant advantages thereof, will be readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols indicate the same or similar components, wherein:

Fig. 1 is a block diagram illustrating the overall architecture of an implementation of the principles of the present invention;

Fig. 2 is a block diagram illustrating a registration by an original equipment manufacture of a portable device with a certificate authority;

Fig. 3 is a block diagram showing the registration of a Internet service provider's registration with a certificate authority;

Fig. 4 is a block diagram showing the registration of a personal computer and a portable device with an Internet service provider;

Fig. 5 is a block diagram showing usage rules governing a database of a right management system;

Fig. 6 is an exemplified format;

Fig. 7 is a block diagram showing the basic architecture for various inputs;

Fig. 8 is a block diagram showing control of outsource import; and

Fig. 9 is a block diagram showing a copy protection system for portable media.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Hereinafter, an preferred embodiment of the present invention will be described in detail with reference to the accompanying drawings.

Fig. 1 illustrates the overall architecture. For the removal of some ambiguities, in this section, we define some terminologies and list up some abbreviated words for a simple description (most of them are those commonly used in PDWG).

First, we have to distinguish the two words, "Portability" and Transferability" of a content.

Portability means that a content in a PM can be played in any PD. Transferability means that portability plus "upload of a content is allowed from a PM to even a LCM", in this case the content's uploadability is to be controlled by *check-in/out system and its transferability status*.

Herein after we use the following abbreviated words.

CA stands for a Certificate Authority (e.g., SDMI, or other trust third party). LCM stands for a Licensed SDMI Compliant Module. PD stands for a SDMI Compliant Portable Device. PDFM stands for a Portable Device Functional Module. ISP stands for an Internet Service Provider (including Content Provider via the Internet). PM stands for a Portable Media (SDMI Compliant Storage Media).

Furthermore, here are presented some notations to be used in the following sections. Even though they are some intricate, we are sure that they would help the readers clearly understand the concrete method we intend. They are relevant to the algorithmic functional modules.

ECC stands for a Elliptic Curve Cryptosystem. $PryKey_A$, $PubKey_A$ stands for a Private Key and Public Key of A (this may be LCM, PD (optional), ISP, CA, ...), respectively. $Cert_{CA}$

($PubKey_A$) stands for a Certificate for a Public Key $PubKey_A$ issued by CA. MK_{PD} stands for the Manufacturer Key within a PD. ID_{MK} stands for the Indicator of a Manufacturer Key. $CK_{PD\text{-}LCM}$ is a secure(secrete) channel key which is setup between PD and LCM. EC_ENC*(key, C)* stands for an Elliptic Curve based Decryption of a ciphertext (encrypted text) *C* by utilizing a private key, *key*. EC_DH*(A, B)* stands for a random secret value (key) shared between A and B by Elliptic Curve based Diffie-Hellman Key Exchanging Protocol. ENC*(key, C)* stands for a Symmetric Key Encryption of a content C by utilizing a secrete key, *key*. *Samsung can support its own Symmetric Key Encryption algorithm, named "SNAKE", that is very effective for both S/W and H/W implementation and it has been world-wide cryptanalized.* DEC(*key*, C) stands for a Symmetric Key Decryption of a ciphertext C by utilizing a secrete key, *key*. Noting that in the above items the Elliptic Curve based Public Key Cryptosystem is just an example as a candidate of Public Key Cryptosystem, and so any public key cryptosystem, for example RSA, can be used instead of it. But we suggest that SDMI compliant EMD System (Electronic Music Distributing System) adopt the ECC System for the next generation PDs, since ECC can be efficiently implemented in such small devices with low cost.

Here, we present the minimum substances (algorithms) that are needed for the insurance of the security of LCM and PD. It is assumed that the content compressing and decompressing CODECs are built in each device in either S/W/-form or H/W-form.

<u>For the LCM</u>

Public Key Cryptosystem (PKC), such as ECC, RSA, ... (ECC is more preferable), is to be used for the secure key setup of LCM, the validity check of ISP's Public Key Certificate, and the

secure channel construction between ISP and LCM. Symmetric Key Encryption Algorithm, such as SNAKE, is to be used for the content encryption, the authentication to a PD, and the secure channel construction between LCM and PD. Secure Chek-in/Chek-out System to be presented in section 6, 7 how to construct this system and how to securely maintain it.

For the PD

Public Key Cryptosystem (PKC) is an optional to PD. Symmetric Key Encryption Algorithm, such as SNAKE, is to be used for the content encryption, the authentication to a LCM, and the secure channel construction between PD and LCM. Manufacturer Key, MK_{PD}, which is the pre-set manufacturer key in a temper resistant area within the PD, is to be used for the secure registration of a PD to LCM.

For the PM

There needs an apparatus or a pre-set special information within a PM to protect contents in it from the dead-copy to another PM. It is desirable, we think, to use the unique ID based approach, that is the method that the manufactures of PM imbed a unique ID of each PM in the write-protected area of it while they manufacture it. This can be considered as a low cost method to dead-copy protection for the first generation PM.

There are four registration mechanisms relative to ISPs, LCMs, and Pds. The manufactures' registration to CA is preceded ahead all the others.

Prior to manufacturing PD, the manufacturers should register to CA to get their manufacturer key, MK_{PD}, and its certificate, $Cert_{CA}(ID_{MK})$, and then produce the SDMI Compliant Portable Devices by using them. Where such registered manufacturer keys are securely stored in CA's DB

and only CA maintains the information. The manufacturer should keep their manufacturer-key and its certificate in safe, maintains the securely, and imbed them in a temper resistant area of PDs while he manufactures PDS.

In Fig. 2, when a manufacturer request its registration to CA, CA certifies it and then generates a manufacturer key, $MK_{PD,}$ and make its certificate data, $CertCA(ID_{MK})$, to deliver them to the manufacturer. At the same time CA generates a random token, T, to make (or update) the Manufacturer Key Information Table (MKIT) for the other ISP-registration. Once after a manufacturer got the data, $\{MK_{PD}, Cert_{CA}(IDMK)\}$, he/she can manufactures PDs by imbedding those secrete data within a temper resistant area of PDs.

Fig. 3 shows how for an ISP to register to CA and what information to get from CA. For an ISP to register to CA, firstly it generates its ephemeral private-public key pair $\{PrvKey_{eph}, PubKey_{eph}\}$ to open a secure channel between CA and itself by EC_DH(CA, ISP). Secondly the ISP gets its semi-permanent private-public key pair $\{PrvKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ and MKIT data appeared these procedures. Noting that ISP's Key Pair should be securely stored, where the host's various system parameters may be used for this goal.

Relating to Fig. 4, the abbreviations stand for as follows. EC_DH(ISP,LCM) represents a random secret value (key) shared between ISP and LCM by Elliptic Curve (Elliptic Curve Cryptosystem) based Diffie-Hellman Key Exchanging Protocol. ENC stands for symmetric Key Encryption of a content by utilizing a secret key. DEC stands for symmetric Key Decryption of a ciphertext by utilizing a secret key. EC-ENC stands for Elliptic Curve Encryption of a content by utilizing a public key. The Encryption is the ElGamal-like public key encryption process. EC_DEC

stands for Elliptic Curve Decryption of a ciphertext (encrypted text) by utilizing a private key. ISP means an Internet service provider including a content provider via the Internet. LCM means a licensed SEMI (secure digital music initiative) compliant module, such as a personal computer. The LCM registration mechanism to an ISP together with PD registration is described. As in Fig. 4, LCM gets the ISP's Public Key Information $\{PubKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ at first and verifies its validity by using the CA's Public Key Information which was already announced or preset within the LCM in a code-imbedded-like method. If the validity of the certificate for the ISP's Public Key is certified, the LCM executes the handshaking protocol to get an ephemeral shared key by utilizing Elliptic Curve based (or other PKC based) Key Exchanging Protocol. Through this secure channel, the ISP can deliver in safe the LCM's permanent private-public key pair for a static secure communication and a secure content transaction between the LCM and the ISP. For a PD to register to the LCM, it has to toss the certificate data for its ID of manufacturer key and the LCM gets this data from the PD to send this to its connected ISP in the encrypted form, $EC\_ENC(PubKey_{ISP}, Cert_{CA}(ID_{MK}))$.

Using this, the ISP can verify the manufacturer key information and can extract its relevant data, $T^*||T$ by looking up MKIP in ISP's DB t transfer it to the LCM in secure manner, *i.e.* by $EC\_ENC(PubKey_{LCM}, T^*||T)$. For the LCM and the PD to setup a shared secret key and to complete the PD registration, the LCM randomly generates their static and secret channel key $CK_{PD\text{-}LCM}$ and sends $ENC(T,CK_{PD\text{-}LCM})||T^*$. Upon receiving this data, the PD can extract the token value T from T^* and using this token the PD can also compute $CK_{PD\text{-}LCM}$. As the PD securely stores this channel key the PD-registration is finished. The Channel Key $CK_{PD\text{-}LCM}$ may be originated from PD instead

of LCM. In this case the PD receives the data T^* from the LCM and gets the token T by decrypting T^* with its manufacturer key. And then the PD generates a random channel key $CK_{PD\text{-}LCM}$ to upload $ENC(T, CK_{PD\text{-}LCM})$ to LCM. The part of the record in MKIT (in LCM) stays in encrypted form by using the LCM's secret key (this key may be LCM's Public Key). In practice, during the PD registration to LCM, the RMS-DB updating token data (UTD or update token data) should be transferred from the PD to LCM (or from the LCM to PD) together with $CK_{PD\text{-}LCM}$ and be set both in the RMS-DB and in the PD. To register a plurality of LCM's, since ISP maintains the private-public key pair of the firstly registered LCM of a user's multiple LCM's, ISP can securely deliver the same key pair to another LCM of the user. To register a plurality of PD's, LCM securely maintains the secret channel key between the LCM and PD, the LCM can securely deliver the same key pair to another PD of the user in the same manner depicted in Fig. 4.

To manage the information CTC={Copyright, Transfer, Check-in/Check-out}, LCM has to maintain the Right Management System DB, named RMS-DB in a secure manner. The Right Management System is described, focusing on the content transaction between LCM and PD. The RMS-DB consists of the Title (or Title-ID), CTC field, Playback Control Status (PCS : the permitted times to play, the amnesty period, ...) and Update Token Data (UTD). This DB stays in LCM in the encrypted form by utilizing LCM's secret key. An important characteristic of the Update Token Data (UTD) is that it is generated from PD whenever any content downloading or uploading session between PD and LCM occurs and that it is also stored in the PD.

Whenever a content is played back at first in LCM, the above right management information of the content's file format is newly registered to the RMS-DB. Once a content is registered to the

RMS-DB, every playback procedure should priory reference to the DB to check the content's validation. The following Fig. 5 shows exemplified implementation for the management rule of RMS-DB when a content downloading occurs. The part of the record in RMS-DB (in LCM) stays in encrypted form by using the LCM's secret key (this key may be $CK_{PD\text{-}LCM}$). The UTD part may have a few number of Updating Token Data depending on the number of a user's own PD's. Noting the part of the record in RMS-DB (in CLM) stays in encrypted form by using the LCM's secrete key (this key may be $CK_{PD.CLM}$).

Noting that the RMS-DB may maintain a finite number of UTDs depending on the limited number of user's own PDs which were already registered to the LCM.

PD Import Control is a layer existing in LCM to import SDMI Compliant contents from ISPs or to import non-SDMI Compliant outsource contents (, e.g. RedBook CDS, DVD, ...). Therefore this should contain three of following capabilities. One is Trans-Coding to make PD decompress the input with its CODEC. Second is Trans-Encrypting to make PD decrypt the input with its Encryption System. Third is to converting the input to SDMI Compliant the format.

PD Interface has two capabilities; Authenticating to PD and opening a secure channel between LCM and PD.

ISP Interface has two capabilities; Authenticating to PD and opening a secure channel

between LCM and PD.

Functional Components in PDFM has LCM Interface and Import Control within PDFM.

LCM Interface has two capabilities; Authenticating to LCM and opening a secure channel between PD and LCM.

Import Control within PDFM has the capability to import an outside analog input and to make it fit to the SDMI Compliant file format. Where the converted SDMI Compliant content should have the binding information to the PD to be played only via the PD.

The SEMI-Compliant file format should contain the following information and should allow extendibility and flexibility:

--Indication of Source Originator--ISP< LCM (CD-ripping, Audio input)< PD (Analog input), Kiosk, ...

--Device IDentifier--LCM_ID,PD_ID, PM_ID

--Algorithm Information Field

--Authentication secret sharing algorithm identifier--EC (Elliptic Curve)-Signature, EC-DH, ...

--Encryption algorithm identifier

--Codec algorithm identifier--MP3, AAC, ...

--Encryption key information of content

--Right Management Field

Right management field contains the Copy, Check-In/Out, Transfer and Playback Control Status, which are to be encrypted by secret key of the device.

--Copy-Never/Copy-Free/No-More-Copy mode

--Check-In/Out mode

--Transfer mode (Transferable or not)

--Playback control information

--Allowable number of times to be played (unlimited or n-times)

--Expiration date

--Amnesty period

--Copyright holder information

--Content description field--Title, Composer, Artist, Record-label, ...

See Fig 6 for an exemplified file format. Dividing the above file format into the following three parts:

--Plain-Header (PH) --{Title-ID, CDF, AIF}

--Secret Header (SH) -- {Device-ID, SOI, CHI, RMF, Content Encryption Key}

--File Body (FB) -- {The Encrypted Content by using the content encryption key in SH}.

The rules to transfer contents securely over ISP-LCM-PD-PM is following.

When an ISP receives content downloading request from a LCM, it confirms the LCM's ID and then downloads the content with the file format of section 7 to the LCM. For the LCM to play the reached content, it follows the following steps in this order. First, finding out the encryption algorithm from the field AIF in PH. Second, using the found out encryption algorithm and LCM's secrete key (private key) to recover the fields in SH. Third, comparing the Device-JD field with its ID. Fourth, from the RMF information confirming the Copy Control Status, Playback Control Status, and Transfer Control Status to register it to its RMS-DB. Fifth, recovering the content encryption key from CEK to recover the real content from FB. If any of these lists does not violate, playing the music.

If it is needed to modify the RMF field, especially the Playback Control Status (PCS), LCM has o replace the data both in the file and in the RMS-DB following the controlling direction.

The procedure for a LCM to download a content to its PD is following steps. First, LCM requests the PD-ID and UTD data to the PD. Second, PD sends the ENC ($CK_{PD\text{-}LCM}$, UTD || PD-ID) to the LCM. Third, LCM recovers the PD-ID and confirms it. Fourth, LCM recovers the UTD and SH part compares them with those in its RMS-DB. If UTD is correct and if any alternation of RMF is needed, the LCM updates the contents of RMF both in RMS-DB and in the file format. Fifth, LCM updates UTD of RMS-DB by newly generated UTD and ENC ($CK_{PD\text{-}LCM,\ UTD}$*) IS TO BE SENT TO THE pd. Sixth, if the Transfer Control Status indicates as "Transfer" then replace it by "Transferred" to the Transfer Control Status filed in RMS-DB not in the file format. Where the

Transfer Control Status field has the three types, "Transfer", "Transferred", and "Transfer-non". Seventh, if the Copy Control Status (CCS) indicates "Check-in", then replace it by "Check-out" to the Copy Control Status field both in RMS-DB and in the file format. Eighth, if the Copy Control Status (CCS) indicates "Copy-Never", the content downloading to a PD is denied. If any of the above lists does not violate, downloading the content to the PD complete.

For contents transaction from PD to PM, in case that unique ID of each PM exists, for a PD to write a content on a PM, it just writes the content on the PM and it recovers the Secret Header (SH) and re-encrypts it by using the unique ID of the PM as an encryption key. For the case that a unique ID of each PM does not exist, fora PD to write a content on a PM, it just writes the content on the PM and it recovers the Secret Header (SH) and re-encrypts it by using a randomly generated key. Where the randomly generated key, say T, is encrypted by a common secrete key, S (this is a present value by the manufacture of the PD), and is also written on a hidden area of the PM.

For the first case of the section 8.3, all contents within the PM can be played by all PDS, but, for the second case, all contents within the PM can be played only by the PDS produced by the manufacturers which adopted this system. Any way it is certain that this system can support the portability of contents via PMs.

As previously we defined in section 3, the "Transferability" is a different concept from the "Portability" of a content. The main difference is that the content with "Transferability" can be not

only played in any PDS but also uploaded to any LCMs, but not in the case of "Portability". Since our system has and manages the Transfer Control Status field both in the RMS-DB and in the file format, out system can support the transferability of a content. If there is marked "Transfer" in the field of a content and if the content is just downloaded to PD, then the LCM downloads it to the PD and replaces "Transfer" by "Transferred" in the relevant field of RMS-DB. Then the content, which has been downloaded to a PD, can no longer be played in the LCM until it is uploaded to the LCM again, but the downloaded content in a PM can be played by any PDS and can be uploaded to another LCM via a PD.

If the Copy Control Status (CCS) of a content contained in a PM indicates "Copy-Free", the content can be uploaded to any LCMs.

As shown in Fig 7, various inputs such as originated from Redbook CD, Audio CD, Super Audio CD, DVD Disk, and analog Device are all allowable to LCM optionally. An analog input to PD is also allowable. The secure import control for those several inputs to LCM or to PD is presented in the next subsections.

As shown in Fig 8, the host device, in which the LCM module exists, has at least the following three layers (two of these exist in the LCM module):

--Authenticated Input API--This API has the roles that confirms the validity of the input and extracts some required information to convert the input into a SEMI Compliant format.

--Validity Check

--If the input data has a watermark, then this API should be able to detect it.

--If the input data takes an encrypted (or scrambled) form, then this API should be able to extract its encryption key and the encryption (or scrambling) algorithm.

--If the input data does not take any protected form, then the API should confirm the validity of written format of the media containing the input data.

--Required data for the API to pass over to the Import Control Layer.

--Information of the media (source) type--Audio CD, DVD Audio, ...

--Information of the originator of the input content

--Information of the content--Title, if any, Player, Artist, ...

--Information of the encryption algorithm if any

--Information of the encryption key if any

--PD Import Control--This Import Control Layer gets a bundle of information from the Authenticated Input API and reconstructs the input content to meet a SEMI Compliant file format by following the rules listed below:

--Copy Control Status--mark "Copy-Never" or "Check-in/Check-out" (optionally)

--Playback Control Status--mark "Times to playback = infinite or N" (N: optional)

--Transfer Control Status--mark "Transfer-Non"

--Mark the "LCM-ID" into the SOI field and Device-ID field of SH (Secret Header)

--If the input content is not encrypted, then generate a random key and encrypt it by the key.

--If the input content takes an encrypted form by other encryption algorithm different from the PD's, then this layer trans-encrypts the content to be played in the PD.

--Public-Key-Encrypt such made secret header part by LCM's public key.

--**PD Interface**--This layer authenticates the connected PD by checking whether the PD has its correct ID and the secret channel key $CK_{PD\text{-}LCM}$. Where the Kerberos Authentication Protocol may be used (refer to: A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, pp. 401-403, CRC Press, 1996).

The Import Control Layer (ILC) within the PDFM makes a SEMI Compliant compressed digital content from the analog input by following the rules listed below:

--Upon reception of each frame of the analog input, the ICL does encoding the frame and does encrypting it by a randomly generated key. If all the frames has been encrypted follow the next steps.

--Copy Control Status--mark "Copy-Never" or "Check-in/Check-out" (optionally)

--Playback Control Status--mark "Times to playback--infinite or N" (N: optional)

--Transfer Control Status--mark "Transfer-Non"

--Mark the "PD-ID" into the SOI field and Device-ID field of SH (Secret Header)

--Encrypt such made secret header part by PD's channel key.

If such converted SEMI Compliant content from the analog input has its SOI field of SH (Secret Header) with marked "PD-ID", then the procedure of writing the content on a PM does not use the unique ID of the PM--This means that such content as made from an analog input to a PD

is not allowed to have the "Portability".

An example for the "Kiosk" may be a shop or a machine that makes a bundle of SDMI Compliant contents into PMs from CD-Ripping, etc. and sells them. Here we regard such Kiosk-like machine as a special LCM with PM-Interface that has a special contraction with some ISPs and groups of copyright holders. Hence, to make a SDMI Compliant PMs from other physical media, the Kiosk-like machine follows the same routines as described in section 9.1 and 8.3.

In this article we proposed a secure copy protection mechanism for the Internet based MOD Services. One of our proprietary modules is relevant to the use of and management of MKIT table appeared in the PD registration procedure. Another one is relevant to the construction of secure Check-in/Check-out system which securely maintains the contents downloading/uploading between LCM and PD.

SAMSUNG Copy Protection Scheme for Portable Media

Referring to Unique ID, ID (Optional feature), PM may optionally support unique ID for first Generation PM. If Unique ID is not supported, Physical address of bad sector of PM is used instead. If unique ID is supported, it should be one-time writeable during manufacturing stage only, and readable only by PD with a special command.

Referring to Channel key, CK, CK is a shared key between LCM and PD. To support portability, CK is not considered as input to function f(). If CK is included, it provides additional

security to the content stored in PM. CK may take various forms depending on the application usage and right management rules.

Referring to Address of Bad Sector of Portable Media, P, the usage of P prevents the playback of illegally copied content from PM to PM by simple "dead-copy".

Referring to Spared Area, a special command known only to the manufacturer needs to be known to access this area.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic view for explaining a system for preventing an illegal copy of digital contents according to an embodiment of the present invention;

FIGs. 2-5 are views for briefly explaining registration requests or digital content reproductions of respective blocks of FIG. 1;

FIG. 6 is a view for showing an example of a file format which is supported by the embodiment of the present invention;

FIG. 7 is a block diagram for showing an output source of digital content processes in a content storage unit of the embodiment of the present invention;

FIG. 8 is a view for showing an output source capable of being additionally connected to the embodiment of the present invention.

Explanation reference number in drawings

10 : authorization recognition means

20 : record/reproduction supply means

30 : content supply unit

40 : PC

50 : portable record/reproduction means

60 : recording medium

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

SUMMARY OF THE INVENTION

FIELD OF THE INVENTION AND DESCRIPTION OF PRIOR ART

The present invention relates to a system for preventing an illegal copy of digital contents, and more particularly to a system for preventing an illegal copy of digital contents which forms secret channels between all the systems connected to users and exchanges contents through the formed secret channels in order to prevent digital contents from an illegal copy.

In recent years, communication environment has rapidly been developed , and each individual can assess a lot of information by using PC with various types of communication equipment.

Therefore, there are digital content suppliers who intend to provide much more digital data to the above first content output units, and the digital content suppliers provide users with digital contents which are document information or audio files such as MP3.

The digital content suppliers require that some fee should be payed in supply of the digital contents.

In the prior art, however, it is difficult to prevent the illegal copy of the supplied digital contents after the digital contents has been supplied to a user.

The present invention relates to a system having a portable recordable medium for preventing an illegal copy of digital contents, and more particularly to a system having a portable recordable medium by using a physical address of bad sector formed the portable recordable medium during manufacturing process of the portable recordable medium and by encrypting a header of the encrypted digital contents stored in the portable recordable medium and recording the encrypted header on a physical address of bad sector of the portable recordable medium. The physical address of bad sector is formed on the portable recordable medium during manufacturing process of the portable recordable medium. This is for preventing an illegal copy of the downloaded digital contents through a terminal after the digital contents has been downloaded.

In recent years, communication environment has rapidly been developed , and each individual can assess a lot of information by using PC with various types of communication equipment or first contents output unit such as internet appliance, PC, PDA, Web Phone, Mobile Phoen,etc.

Therefore, there are digital content suppliers who intend to provide much more digital data to the above mentioned first content output units, and the digital content suppliers provide users with digital contents which are document information, video information, song words, character display such as movie caption, or audio files such as MP3, Aac, G2, etc. Various types of codec provided by this invention can be downloaded and recorded in a potable medium which can be played on a

portable medium player or portable medium terminal.

However, it is difficult to prevent the illegal copy of the supplied digital contents or the codec recorded on the portable medium if the portable medium is copied after the digital contents has been supplied to a user and recorded on the portable medium.

At this time, the digital contents which are used in the present invention mean all data including audio, video data, as well as character data such as song words, movie caption, and the like to be provided through internet.

In particular, the MP3 which is the audio data of the above digital contents is downloaded to the first content output unit as well as the second content output unit such as an MP3 player and then reproduced.

In the meantime, the MP3 is downloaded to a content storage unit such as a smartmedia card built in the first content output unit, and the MP3 downloaded in the content storage unit is reproduced through the second content output unit.

However, as stated above, there is a drawback in that digital data downloaded to the first and second content output units and the content storage unit is easily copied to be illegally distributed

TECHNICAL OBJECT OF THE INVENTION

This invention provides a system for preventing an illegal copy of digital contents which is downloaded and uploaded the digital contents. The system forms secret channels between all the systems connected to users and exchanges contents through the formed secret channels in order to prevent digital contents from an illegal copy.

The present invention provides a system having a portable recordable medium for preventing an illegal copy of digital contents, and more particularly to a system having a portable recordable medium by using a physical address of bad sector formed the portable recordable medium during manufacturing process of the portable recordable medium and by encrypting a header of the encrypted digital contents stored in the portable recordable medium and recording the encrypted header on a physical address of bad sector of the portable recordable medium. The physical address of bad sector is formed on the portable recordable medium during manufacturing process of the portable recordable medium. This is for preventing an illegal copy of the downloaded digital contents through a terminal after the digital contents has been downloaded.

SUMMARY OF THE INVENTION AND DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Accordingly, in order to solve the above problem, it is an object of the present invention to provide a system for preventing an illegal copy of digital contents for preventing from an illegal copy and distribution a digital content downloaded by forming a secret channel between all the system mutually connected as users download and reproduce the digital content.

In order to achieve the above object, the present invention includes an authorization recognition unit for generating a first authentication qualification key and a first authentication qualification key data, which may be encrypted, and for generating a manufacturing key and

manufacturing key information for reproducing and outputting the encrypted digital contents supplied or supplying in response to a registration request signal inputted from external, a portable terminal supplying means requesting the registration request signal and receiving the manufacturing key and manufacturing key information, a content supply unit for transmitting the registration request signal to the authorization recognition unit, for storing the first authentication qualification key and the first authentication qualification key data inputted from the authorization recognition unit in order to be authorized to supply the encrypted digital contents, and for generating a second authentication qualification key and a second authentication qualification key data, and a PC for outputting the third registration request signal to the content supply unit, for storing the second authentication qualification key and the second authentication qualification key data inputted from the content supply unit, and for receiving a public key, public key information and digital contents.

Further, in order to achieve the above object, the present invention includes an authorization recognition unit for forming a first table having a manufacturer key, a manufacturer key data and a second table having a token, information relating to an encrypted token by using the manufacturer key, identification of a portable device or terminal and forming a pair of table with the first table in response to a first registration request signal inputted from external, for generating a first table and a second table by using the manufacturer key and the manufacturer key data, and for generating a first authentication qualification key and a first authentication qualification key data in response to the second registration request signal inputted from external, a portable terminal unit for outputting the first registration request signal to the authorization recognition unit and for storing the

manufacturer key and the manufacturer key data inputted from the authorization unit, a content supply unit for outputting the second registration request signal to the authorization recognition unit, for storing the first authentication qualification key, the first authentication qualification key data, and the second table, and for generating a second authentication qualification key and a second authentication qualification key data in response to a third registration request signal inputted from external, a first content output unit like as a PC for outputting the third registration request signal to the content supply unit in order to receive the digital contents and output the received digital contents, for storing the second authentication qualification key and the second authentication qualification key data such as Public key and Public Key information inputted from the content supply unit, for outputting the manufacturer key data inputted from external to the content supply unit, for encoding and outputting the manufacturer key detected from the second table in response to the manufacturer key data, and a second content output unit such as a portable terminal for storing the manufacturer key and the manufacturer key data inputted from the authorization recognition unit, for outputting the manufacturer key data to the content supply unit through the first content output unit, and for receiving the manufacturer key information of the second table, which is encrypted, supplied from the PC in order to judge if the stored manufacturer key is authenticated.

Further, in order to achieve the above object, the present invention includes a content supply unit for supplying an encoded digital content, a first content output unit including a database which has a reproduction data of the digital content downloaded from the content supply unit, encoding the database by using the third channel key for storage, interpreting the reproduction data of the digital

content inputted from external by using the third channel key to be compared with a reproduction data of the database, to thereby judge if an illegal copy of the digital content is performed, and a second content output unit for updating the reproduction data of the digital content stored in advance by interpreting the reproduction data of the digital content inputted from the first content output unit by using the third channel key, and transmitting the updated reproduction data of the digital content to the first content output unit.

Hereinafter, an preferred embodiment of the present invention will be described in detail with reference to the accompanying drawings.

FIG. 1 is a schematic view for explaining a system for preventing an illegal copy of digital contents according to an embodiment of the present invention, in which the structure is as follows.

An authorization recognition unit 10 generates a manufacturer key and a manufacturer key data in accordance with a first registration request signal inputted from a record/reproduction apparatus supply unit as a portable terminal supply means as described later, and outputs a manufacturer key and a manufacturer key data to the record/reproduction apparatus supply unit. Further, the authorization recognition unit 10 uses the manufacturer key and a manufacturer key data forming first and second tables , and generates a first authentication qualification key and a first authentication qualification key in accordance with a second registration request signal inputted from a content supply unit.

A portable terminal supplying means 20 outputs the first registration request signal to

authorization recognition unit 10 and receiving the manufacturer key and a manufacturer key data generated by authorization recognition unit 10 in accordance with the first registration request signal.

A content supply unit 30 outputs the second registration request signal to the authorization recognition unit, stores the first authentication qualification key, the first authentication qualification key data, and the second table, and generates a second authentication qualification key and a second authentication qualification key data in response to a third registration request signal inputted from external.

A PC 40 as a first content output unit outputs the third registration request signal to the content supply unit 30 in order to receive the digital contents and output the received digital contents, stores the second authentication qualification key and the second authentication qualification key data such as Public key and Public Key information inputted from the content supply unit, outputs the manufacturer key data inputted from external to the content supply unit, encodes and outputs the manufacturer key detected from the second table in response to the manufacturer key data.

A portable terminal 50 as a second content output unit stores the manufacturer key and the manufacturer key data inputted from the authorization recognition unit, outputs the manufacturer key data to the content supply unit through the first content output unit, and receives the manufacturer key information of the second table, which is encrypted, supplied from the PC in order to judge if the stored manufacturer key is authenticated.

In the meantime, the first authentication qualification key and the first authentication qualification key mean a public key, a public key data, and a private key

of the content supply unit 30 generated from the authorization recognition unit 10.

Further, the first table, as shown in FIG. 2, contains a manufacturer key data(Cert(MK_{PD})), the manufacturer key(MK_{PD}), and an identifier(ID_{MK}) corresponding to the manufacturer key data and the manufacturer key, and is stored in only the authorization recognition unit 10. Further, the second table is generated from the authorization recognition unit 10 and outputted to the content supply unit 30, and contains the identifier(ID_{MK}), data(ENC(MK_{PD}, T)), and a token(T) which encodes the manufacturer key by using the token.

At this time, he authorization recognition unit 10 forms a first channel key(k) which can be shared with the content supply unit 30 in accordance with the second registration request signal 31 inputted from the content supply unit 30, and outputs the first authentication qualification key and the first authentication qualification key data 11 which is encoded into the content supply unit 30 through a secrete channel formed by the first channel key(k).

The first channel key is a key generated from encryption of the authorization recognition unit 10 by using data which the content supply unit 30 has.

Hereinafter, an preferred embodiment of the present invention will be described in detail with reference to the accompanying drawings.

FIGs. 2-5 are views for briefly explaining the flow of registration requests by respective blocks or Keys and Key information or data for the digital content reproductions by respective blocks of FIG. 1.

The portable terminal supply unit 20 outputs the first registration request signal to the authorization recognition unit 10 in order to register the portable device or terminal to the authorization recognition unit 10.

The authorization recognition unit 10 generates and transmits manufacturer key MK_{PD} and the manufacturer key data ($Cert_{CA}(MK_{PD})$, which is possessed by each designated portable device for its own use, to portable terminal supply unit 20 as a record/reproduction apparatus.

Therefore, portable terminal supply unit 20 stores the received manufacturer key and the manufacturer key data into an internal memory like as a tempery resistant area of portable terminal supply unit 20 during manufacturing portable terminal supply unit 20. The stored manufacturer key and the manufacturer key data of portable terminal supply unit 20 can not be noticed by other users.

The authorization recognition unit 10 generates the manufacturer key and the manufacturer key data to be transmitted to portable terminal supply unit 20 and generates a token randomly.

The authorization recognition unit 10 includes two tables. The first table is possessed by the authorization recognition unit 10, which includes manufacturer key and the manufacturer key data information.

The second table is a manufacture key information table which is transmitted from authorization recognition unit 10 to content supply means 30 and is a table having identifier of the portable terminal, the token encrypted by the manufacture key, and information for the token.

Therefore, portable terminal 50 which is manufactured by the portable terminal supply unit 20 is authorized by authorization recognition unit 10 to store the downloaded, encrypted digital contents.

In addition, The content supply unit 30 outputs the second registration request signal in order to obtain the authorization.

Then, Key and Key data information is generated between content supply unit 30 and authorization recognition unit 10 shown in Fig. 2..

In accordance with the request signal from content supply unit 30, authorization recognition unit 10 generates a private key $PrvKey_{eph}$ and a public key $PubKey_{eph.}$

A pair of keys and key information $\{ PrvKey_{isp,} PubKey_{isp,} Cert_{CA}(PubKey_{ISP} \}$ are generated and stored in content supply unit 30, and two tables are formed in dependence with the manufacture key.

Because content supply unit 30 and authorization recognition unit 10 have a channel formed by a co-owned key EC_DH(CA,ISP), the channel formed between content supply unit 30 and authorization recognition unit 10 provides a safe way to communicate each other without allowing an illegal copy of the downloaded information through the channel.

Authorization recognition unit 10 transmit a encrypted key and key information to content supply unit 30 through the channel in order to co-own the key and key information. Content supply unit 30 decrypts the encrypted key and key information by using co-owned key and stores the key and key information. Set up between content supply unit 30 and authorization recognition unit 10 is finished.

After the setup of content supply unit 30 and authorization recognition unit 10, PC 40 transmits a request signal to content supply unit 30 to receive the encrypted digital contents. Content supply unit 30 transmits its public key and public key information $PubKey_{isp,}$ $Cert_{CA}(PubKey_{ISP})$ to

PC 40. PC 40 stores the received republic key and public key information $PubKey_{isp}$, $Cert_{CA}(PubKey_{ISP})$.

A key generated by EC_DH(ISP,LCM) is co-owned by content supply unit 30 and PC 40 and forms a channel between content supply unit 30 and PC 40. PC 40 can receive the digital contents from content supply unit 30 through the channel.

Public key and public key information is transmitted from content supply unit 30 to PC 40 through the channel. Setup between content supply unit 30 and PC 40 for downloading the digital contents is finished.

When a request signal is transmitted from potable terminal 50 to PC 40, potable terminal 50 transmits the manufacture key, which has been received from Authorization recognition unit 10 and stored in the memory of potable terminal 50, with the encrypted Public key, which is received from content supply unit, to content supply unit 30 through PC 40.

Content supply unit 30 decrypts the encrypted information and compares the encrypted information with the information of the second table. If the encrypted information is identical to the information of the second table, content supply unit 30 encrypts the content of the table and transmits the encrypted information to PC 40. PC 40 decrypts the encrypted information to obtain the information of the token.

At this time, a channel key is randomly generated in PC, is maintained in confidential. PC 40 encrypts the channel key and transmit to portable terminal 50 the encrypted channel key by using the decrypted token information.

Portable terminal 50 reads the token information from the information of the table received

from content supply unit 30 by using the manufacture key.

The registration process is finished when the channel key obtained by decrypting the encrypted information by using the token information and the channel key is co-owned by PC 40 and portable terminal 50.

Therefore, all the units and terminals in this system are authorized to transmit and receive the encrypted digital contents between the units and terminals.

PC 40 includes a data base such as RMS-DB (Right Management System-Data Base) described in Fig. 6 for preventing the illegal copy of the digital contents when PC 40 transmits the digital contents received from content supply unit 30.

The above data base is applied for processing the digital contents transmitted between PC 40 and portable terminal 50. Referring to the structure of the data base. The database contains an identifier data area of the digital content, an updated token data area, a data area for checking a present state of the digital content, and a reproduction control data area.

Further, the database is stored in PC 40 in an encoded form by the secret channel key which PC 40. The most important area in the database is the updated token area, and the updated token area has different values when the updated token area downloads a digital content from PC 40 to portable terminal 50, or uploads the digital content from portable terminal 50 to PC 40. At this time, the updated token is transmitted to PC 40 through portable terminal 50 to update the stored token in PC 40.

That is, data registered in the database of PC 40 becomes different every time PC 40

reproduces, downloads, or updates a digital content downloaded into PC 40. Therefore, PC 40 checks the registered data in the database if users legally use the digital content in the case that a request signal for reproduction, download, or upload of the digital content is inputted by the users.

Further, in the case that the digital content is downloaded or uploaded between PC 40 and the portable terminal 50, an area is checked which has data for checking a present state of the digital content and which is the second area of the database.

That is, since PC 40 checks the third area, when the portable terminal 50 downloads a digital content downloaded from the content supply unit to the second content output unit, the selection of a copy form or a transmission form can be read.

Further, by checking check-in/check-out data included in the second area, the transmission state of the digital content can be read. That is, the check-in data means that a digital content is not downloaded from the content supply unit to the portable terminal 50.

The check-out data means that the digital content is a downloading state from the portable terminal supply unit 20 to the portable terminal 50, or that the downloaded digital content is again uploaded to PC 40.

The last area of the database is a reproduction control data area and contains data for reproduction times of a digital content, a reproduction expiration period of the digital content, and an amnesty period of the digital content.

Here, the reproduction times of the digital content is a value which is established when a digital content is provided from the content supply unit 30 to PC 40 and which controls the reproduction times by counting down one by one every time the digital content is downloaded.

Further, the reproduction expiration period of the digital content does not mean the reproduction of the digital content and the control of the output state, but a period established by the content supply unit 30, and the digital content downloaded from the content supply unit 30 to PC 40 can be reproduced in the period as stated above.

Lastly, the amnesty period of the digital content enables the digital content downloaded from the content supply unit 30 to PC 40 to be reproduced irrespectively of the reproduction times of the digital contents or the expiration period.

As stated above, if the content supply unit 30 accepts a download request of a digital content of PC 40, the content supply unit 30 firstly identifies the ID of PC 40 as a first content output unit, judges as PC 40 legally connected to the content supply unit 30, and downloads a digital content having a file format embodied by the secret system to PC 40.

The file format having a digital content transmitted to PC 40 from the content supply unit 30, as shown in FIG. 6, contains a title ID field, a content description field (CDF), algorithm identifying field (AIF), an indicator of source originator field (SOI), a copyright holder information field (CHI) indicating a copy holder information, a right management field (RMF), a content encryption key (CEK), and a digital content field encoded to a content encryption key.

The content description field has data such as a digital content composer, a singer, a record label or the like.

The algorithm identifying field denotes an algorithm employed in the secret system embodied in the present invention, and there are ECC, SNAKE, CODEC and the like in the algorithm.

The SOI field has one of data of ISP_ID denoting an identifier of a content supply unit 30 of the present invention, LSP_ID denoting an identifier of the first content output unit 40, PD_ID denoting an identifier of portable terminal 50.

Therefore, in the case that PC 40 downloads and reproduces a digital content having the format as stated above, firstly an algorithm encoded from the AIF field is identified, and the authentication qualification of PC 40 is recovered by using the identified encryption algorithm.

Further, the identifier which PC 40 has and the identifier in the SOI field of the file format are compared to check if there is correspondence between the two. In the case of correspondence, the copy control state from the RMF data, the reproduction control state, and the transmission control state are identified to register them in the database(RMS-DB) which the first content output unit 40 has.

After the above process is performed, a digital content encryption key is extracted by using a CEK field, and the encoded digital content is interpreted by using the encryption key.

At this time, in the case that PC 40 does not violate any one of the above, the content supply unit 30 judges that PC 40 is legal, and downloads the digital content.

In the case of changing the RMF field of the file formats, in particular the reproduction control state, PC 40 replaces the reproduction control state data in two places of the database(RMS-DB) and the file format with desired data.

Further, as stated above, in the case that a digital content downloaded from PC 40 is again downloaded to t portable terminal 50, the following precesses are required.

Firstly, PC 40 receives the UTD data which portable terminal 50 of the identifier of the

second content output unit by a request to portable terminal 50.

Therefore, portable terminal 50 encodes the UTD into the third channel key($CK_{PD\text{-}LCM}$) shared with PC 40 and the third channel key($CK_{PD\text{-}LCM}$) is transmitted to PC 40 together with the identifier of the second content output unit. At this time, PC 40 identifies data transmitted from portable terminal 50 and extracts the identifier of portable terminal 50 and the UTD from the transmitted data by using the channel key($CK_{PD\text{-}LCM}$) shared with portable terminal 50, and compares the extracted identifier of portable terminal 50 and the UTD with data registered in the database.

If the UTD is unchanged and the RMF is changed, the first content output unit 40 updates the two places of the database and the file format to the changed RMF.

That is, PC 40 updates the database to a newly generated UTD, and the updated UTD is encoded by the channel key($CK_{PD\text{-}LCM}$) and the encoded channel key($CK_{PD\text{-}LCM}$) is transmitted to portable terminal 50.

In the meantime, PC 40 transmits a digital content to portable terminal 50, and data of an initial transmission control state field is 'Transfer'. As the digital content is transmitted to portable terminal 50, data of the transmission control state field is changed to 'Transferred'. As stated above, changed data of the transmission control state field is updated in the database(RMS-DB), and is not changed in the file format. At this time, the transmission control state field has three types of 'Transfer', 'Transferred', and 'Transfer-non'.

Next, as a digital content is transmitted to portable terminal 50 from PC 40, data for the copy control state field is initially set to the check-in in the database as well as in the file format, but after the digital content is transmitted, the data for the copy control state field is changed to the check-out

both in the database and the file format.

If the data for the copy control state field is set to 'Copy-never', users using the system of the present invention can not download the digital content of PC 40 to portable terminal 50.

If the above processes are correctly performed, the digital content is downloaded to portable terminal 50.

Hereinafter the process of the digital contents between portable terminal 50 and recording medium 60 as a content storage medium is explained for preventing an illegal copy in downloading a digital content, which portable terminal 50 has, to the content storage unit 60.

Firstly, if there is the its owned ID in the content storage unit 60, portable terminal 50 record the digital contents which is encrypted by using the ID.

Secondly, if there is the its owned ID in the content storage unit 60, portable terminal 50 record the digital contents which is encrypted by using randomly generated key.

The randomly generated key T is encrypted by using a key S of the general secret key which is predetermined by the manufacturer of the portable terminal.

The encrypted T is recorded on the hidden area of the content storage unit 60.

As described above, in first case, all digital content stored in content storage unit 60 may be reproduced in portable terminal 50. In second case, all digital content stored in content storage unit 60 may be reproduced in only the portable terminal 50 which is produced by the designated manufacturer having this system.

The portable terminal 50 transmits to the content storage unit 60 an encoded digital content to be recorded in the content storage unit 60 and an encoded reproduction data to reproduce the digital content. At this time, another encryption of data necessary to produce the encoded digital content is performed as follows. That is, portable terminal 50 contains a random number generation unit (RNG) for randomly generating a number, and a function process unit(F) for function-processing various inputs and generating predetermined values which only the content storage unit 60 can have. At this time, values inputted to the function process unit(F) are a random number, a channel key, and a bad sector address and an inherent number which the content storage unit 60 inherently has. Further, another encryption of an encoded digital content reproduction data is performed by using function values generated in the function process unit(F).

A digital content referred to in the present invention is downloaded from PC 40 to portable terminal 50 and the content storage unit 60, or uploaded from portable terminal 50 to PC 40.

This is denoted by checking a field indicating transmission control state data of file format data which is provided from the database and the content supply unit 30.

If, as stated above, 'transfer' is indicated as a result that the first content output unit 40 checks the database and the transmission control state data field of the file format, PC 40 can download a digital content to portable terminal 50, if the digital content is downloaded from PC 40 to portable terminal 50, 'transfer' is changed to 'transferred' in the database and the transmission control state data field of the file format and the changed data is transmitted to portable terminal 50.

Further, since the digital content downloaded to portable terminal 50 is not in PC 40, in order to be again reproduced in PC 40, the digital content is again uploaded from portable terminal

50 to PC 40.

However, the digital content downloaded to the content storage unit 60 from PC 40 can be reproduced in an arbitrary second content output unit 50. Further, the digital content downloaded to the content storage unit 60 is uploaded to another first content output unit 40 through portable terminal 50.

Further, various input devices are additionally connected to PC 40 and portable terminal 50 applied to the present invention, and such input devices are shown in detail in FIG. 8.

That is, the input devices which can be additionally connected to PC 40 and portable terminal 50 can be CD such as RedBook CD, audio CD, super audio CD, DVD Disk, and analog input, and the like.

The audio signal inputted through the input devices is inputted to PC 40, and encoded according to a system supported in the present invention, and then transmitted to portable terminal 50, or transmitted to the content storage unit 60 to be reproduced through portable terminal 50.

FIG. 8 is a view for showing an output source of Fig. 7 capable of being additionally connected to the embodiment of the present invention.

As shown in FIGs, applied program interface (API) of the first content output unit (indicated as 'Host') checks if data inputted through the CD, EMD (content provided over internet), PM, DVD, and the like(hereinafter, referred to as 'input devices') can be reproduced in a system supported in the present invention.

Therefore, if the data can be reproduced in the system supported in the present invention, the API converts data inputted from the input devices to a format which can be reproduced in the system.

In the meantime, as a method which data can be reproduced in the system supported in the present invention as stated above, first, in the case that the input devices are the super CD or DVD, data which checks if data recorded on the storage medium can be copied is in an area out of data area. The API detects the area and uses the data when converting a signal inputted to PC40 to a file format supported in the present invention.

Secondly, in the case that the input device is the EMD and data inputted through the EMD has an encoded format, the API detects an encryption key and an encryption algorithm and uses the data when converting a signal inputted to the first content output unit 40 to a file format supported in the present invention.

Thirdly, if the input device is a general analog input, the API encodes inputted data according to a system supported in the present invention.

In the meantime, the API checks if an input device and data inputted from the input devices are suitable for the system and transmits the following data to the import control layer.

First, data for the type of a storage medium, for example, data for a type of an input device such as audio CD, DVD and the like, second, data for an initial form of data inputted to PC 40 from an input device, for example, data for a title, a player, a singer and the like, third, data for an encryption key which is data for an encryption algorithm.

At this time, the data is transmitted to portable terminal 50 from PC 40 through the first

interface part. Further, the data inputted from the third interface part of portable terminal 50 is inputted to the import control layer of the second content output unit to be restructured in a file format.

That is, the file format formed in the import control layer of portable terminal 50 indicates data for a storage medium in the title-ID field, data for initial data inputted to an internet appliance from an input device for the CDF, data for an encryption algorithm outputted to the import control layer from the API of the first content output unit for the AIF, LCM-ID in the Device-ID field and SOI field, data for a copyright protection in the CHI field, and following data for the RMF.

First of all, 'copy not available' is indicated for the copy control state, 'check-in/check-out' is selectively indicated for the download/upload, 'reproduction times=no limit or predetermined times' is selectively indicated for the reproduction control state, and 'transmission not available' is indicated for the reproduction control state since the copy control state is 'copy not available' .

Next, CEK=k field which is a field indicating data for an encryption key, if an inputted digital content is not encoded, randomly generates a key(k), and a digital content inputted from the first content output unit is encoded by the key(k) and indicated in the last field (ENC(k, Content)).

At this time, PC 40, if data inputted through an input device is encoded, judges what algorithm is used for encryption, and checks an encryption algorithm which portable terminal 50 to transmit an encoded digital content has.

Accordingly, if two algorithms are not matched, the first content output unit 40 interprets an encoded digital content and performs a trans-crypted process which again encodes the digital content with encryption/decryption algorithm which portable terminal 50 has.

In the meantime, in the file format formed through the process, there is a secret header portion from the Device-ID field to the field which indicates the encryption key. The secret header is encoded by the second authentication qualification key($PubKey_{LCM}$) which the first content output unit 40 has.

In the meantime, the first interface part in PC 40 checks if portable terminal 50 has an identifier and the third channel key($CK_{PD\text{-}LCM}$) and identifies if the qualification is an authenticated second content output unit 50.

In the meantime, an analog input inputted to portable terminal 50 is inputted to the import control layer of a PDFM (PD Functional Module) in the portable terminal 50, and the analog input is converted to a file format supported in the present invention by a process described later.

Here, the import control layer, if the analog input is received by frame unit, first encodes the frame, encodes the encoded frame by using a randomly generated key, and if all frames are encoded, a file format is formed for preventing a copy for an encoded analog input.

In order to prevent an illegal copy as in data indicated for RMF, an encoded analog input has a detailed information.

That is, 'copy not available' is indicated for the copy control state, 'check-in/check-out' is selectively indicated for the download/upload, 'reproduction times=no limit or predetermined times' is selectively indicated for the reproduction control state, and 'transmission not available' is indicated for the reproduction control state.

Further, data of the Device-ID field and the SOI field which are prepared before the RMF is indicated as 'PD_ID'.

The secret header portion generated via the above process is encoded by the third channel key ($CK_{PD\text{-}LCM}$) which the second content output unit 50 has.

At this time, portable terminal 50 transmits the encoded digital content to the content storage unit 60, since a digital content which is transmitted to the content storage unit 60 does not indicate the SOI field data as an identifier which the content storage unit 60 has but as 'PD-ID' as stated above, the digital content can not be reproduced via arbitrary second output unit 50.

That is, a digital content recorded on the content storage unit can be reproduced only in portable terminal 50 which has the same identifier as 'PD-ID' data of the SOI field contained in the content.

Accordingly, as stated above, in the present invention, entire system shares a channel key between units performing mutual communication, forms a safe channel, mutually transmits and receives a digital content, and prevents illegal users from taking the digital content on the way. Further, even though legal users legally downloads a digital content, since the second content output unit has the above structure, illegal copy of a digital content between the second content output unit as well as the content storage unit is prevented.

The kiosk generates a registration request signal for selling an encoded digital content by the content supply unit 30 through a PC. Therefore, the content supply unit 30 provides to the kiosk the storage medium having a digital content encoded by a system supported in the present invention according to the registration request signal, and the kiosk receives fees from users and transmits a digital content stored in the storage medium. Kiosk is a store or vending machine selling a recording medium or digital content which is reproduced in this system. Machine on Kiosk is regarded as a

PC having an interface of the digital content storage medium. The recording medium interface can be used by any one having a supply agreement with intellectual property right owner or the digital content supply unit.

In order to achieve the above object, the present invention includes an illegal copy protecting system having a portable terminal transmitting the encrypted digital content which is received from digital content supply unit to a digital content storage medium. In another preferred embodiment, the digital content transmitted from LCM ca be stored directly in the digital content storage medium. The system includes a portable terminal processing the random number stored in spare area of the digital content storage medium such as physical address of the bad sector of the digital content storage medium and transmitting the encrypted header of the digital content by using the processed value of the random number, and a digital content storage medium reading and transmitting the physical address by using the portable terminal and storing the number as a key value randomly generated by the portable terminal, and storing the encrypted header information encrypted by the resultant value and the encrypted digital content as sector data.

Portable terminal 100 process the random number stored in spare area of the digital content storage medium such as physical address of the bad sector of the digital content storage medium and channel key stored in the portable terminal and transmits the encrypted header of the digital content by using the processed value.

The portable terminal can download and reproduce the MP3 music file.

Storage medium 200 reads and transmits the physical address by using the portable terminal

and storing the number as a part of the input function process F randomly generated by the portable terminal, and stores the encrypted header information encrypted by the resultant value and the encrypted digital content as sector data.

The storage medium 200 is a general medium including a smart media.

More details are explained hereinafter with drawings showing a system having a portable storage medium for protecting a illegal copy.

Portable terminal 100 downloads the digital content from the content supply unit or PCLCM.

Portable terminal 100 owns a secret key like as channel key CK with the content supply unit or PCLCM to form a channel between portable terminal and the content supply unit or PCLCM .

Portable terminal 100 stores in the sector data area of the storage medium the digital content received through the input port of the portable terminal.

Portable terminal 100 encrypts the header portion of the digital content in order to prevent the digital content stored in the storage medium from being illegal copied in other storage medium. The header portion of the digital content is encrypted as a CK and transmitted from LCM to portable terminal 100. At this time, what generates the key for encryption is the function process means 110.

Function process means 110 receives as an input the physical address of the bad sector transmitted from storage medium 200 and receives as an input the random number through the random generating means 120. The random number is stored in the storage medium.

Therefore, function process means 110 receive the commonly owned key generated by LCM, random number, and the physical address of the bad sector of the storage medium for function processing and storing in the sector data area of the storage medium the encrypted header portion of the digital content by inputting the resultant value into the encryption and decryption means 130.

It is optional to encrypt the header of the digital content by function processing after receiving all of the commonly owned key, random number, and the physical address of the bad sector or one of the commonly owned key, random number, and the physical address of the bad sector.

EFFECT OF THE INVENTION

As stated above, this invention provides the effect on protecting illegal copy between portable terminals because any portable has the above described same system and all systems consisting this invention commonly own the channel key formed between systems communicating each other in order to prevent the authorized user from making a copy of the legally downloaded digital content.

Even if the storage medium is copied to another storage medium, the digital content in the another storage medium can not be reproduced from the another storage medium. Therefore, this invention provides the effect on basically protecting illegal copy.

As stated above, preferred embodiments of the present invention are shown and described.

Although the preferred embodiments of the present invention have been described, it is understood that the present invention should not be limited to these preferred embodiments but various changes and modifications can be made by one skilled in the art within the spirit and scope of the present invention as hereinafter claimed.